UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

SYNOPSYS, INC.,

Plaintiff,

v.

UBIQUITI NETWORKS, INC., et al.,

Defendants.

Case No. 17-cv-00561-WHO (LB)

ORDER THAT TAIWANESE COMPUTERS ARE NOT PER SE OUTSIDE THE SCOPE OF DISCOVERY

Re: ECF Nos. 99, 105, 109, 110

INTRODUCTION

This lawsuit centers on allegations by plaintiff Synopsys, Inc. ("Synopsys"), a software company, that the defendants (collectively, "Ubiquiti") "pirated" its software by installing it on Ubiquiti's computers and then using counterfeit license keys to run the software without obtaining a valid license. Among other claims, Synopsys alleges that Ubiquiti (1) circumvented technological measures that control access to copyrighted software, in violation of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a)(1), and (2) committed fraud in representing to Synopsys that it was interested in entering into a license agreement to obtain Synopsys software when it in fact was planning to use counterfeit license keys. Synopsys issued discovery requests to "forensically inspect" Ubiquiti's computers for evidence to support its claims. Ubiquiti objects to Synopsys's requests.

The parties' discovery dispute involves two issues: (1) relevance and (2) burden. The parties' briefs focus almost entirely on relevance. Ubiquiti's main argument is that all but two of the computers at issue are located outside the United States, the DMCA and U.S. copyright law do not impose liability for activity that occurred outside the United States, and hence the computers outside the United States are not relevant to Synopsys's claims and should be excluded from discovery. Synopsys disagrees with Ubiquiti's factual and legal contentions. As for burden, the court previously instructed the parties to meet and confer on the specifics of an appropriate inspection protocol and, if they were unable to agree on a solution, to submit a joint letter brief with their respective positions on how inspection would work, exactly what would be inspected, and what burdens that inspection might impose.[1] The parties have not reached an agreement or submitted a joint letter brief with this information.[2]

The court held a hearing on January 25, 2018. Because the parties did not raise burden arguments before the hearing, this order does not address burden issues and addresses only the parties' relevance arguments. The court holds that Ubiquiti computers are not per se outside the scope of relevant discovery merely because they are located outside the United States.

STATEMENT

1. Synopsys Claims That Its Data Shows That Ubiquiti Circumvented Its Software's License-Key-Protection System Approximately 39,000 Times

Synopsys is a world leader in semiconductor design software.[3] Ubiquiti develops networking technology and, among other things, designs semiconductor chips for use in its products.[4]

Synopsys alleges that Ubiquiti downloaded Synopsys electronic design automation ("EDA") software onto Ubiquiti computers.[5] Synopsys alleges that its software will not run without a

[1] *See* Order – ECF No. 104 at 2, 5–6. Citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

[2] *See* Letters – ECF Nos. 111, 114, 117–119.

[3] Joint Case Mgmt. Statement – ECF No. 98 at 2.

[4] *Id.*

[5] *Id.* at 3.

United States District Court
Northern District of California

license key and that Ubiquiti has been using counterfeit license keys since at least February 2014 to access and run Synopsys software on its computers without obtaining a valid license.[6]

This software has a built-in feature: according to Synopsys, its software transmits basic information about computers that use counterfeit license keys, such as the computers' MAC addresses, IP addresses, and server host names, back to Synopsys.[7] The parties refer to this transmission as "call-home" or "phone-home" data. Synopsys claims that call-home data here shows that Ubiquiti used counterfeit license keys over 39,000 times to access Synopsys software.[8]

2. Ubiquiti Installed Synopsys Software on Taiwanese Computer Servers, and U.S. Employees Remotely Connected to Those Servers to Run Synopsys Software

Ubiquiti acknowledges that it installed Synopsys software on a "storage array" in Taiwan that is accessed through three computer servers located in Taiwan.[9] Ubiquiti employees can access and run the software by using their local laptops or desktops and remotely connecting to the servers.[10]

Ubiquiti also acknowledges that when its employees remotely access its servers to run Synopsys software, Synopsys's call-home data reports the MAC address and host name of the server (or virtual machines running on the server), not the MAC address or host name of the employee's local computer.[11] Similarly, the call-home data reports the user name of the account profile on the server that the employee uses to remotely log on, not the user name of the account profile the employee has on his local computer.[12] Additionally, Synopsys asserts that the call-home data reports the IP address and the country location of the server, not the IP address or the country location of the end user.[13]

[6] *Id.* Ubiquiti disputes that a license key is necessary to run Synopsys software. *Id.*

[7] Joint Letter Br. – ECF No. 99 at 2.

[8] Joint Case Mgmt. Statement – ECF No. 98 at 3; Joint Letter Br. – ECF No. 99 at 4.

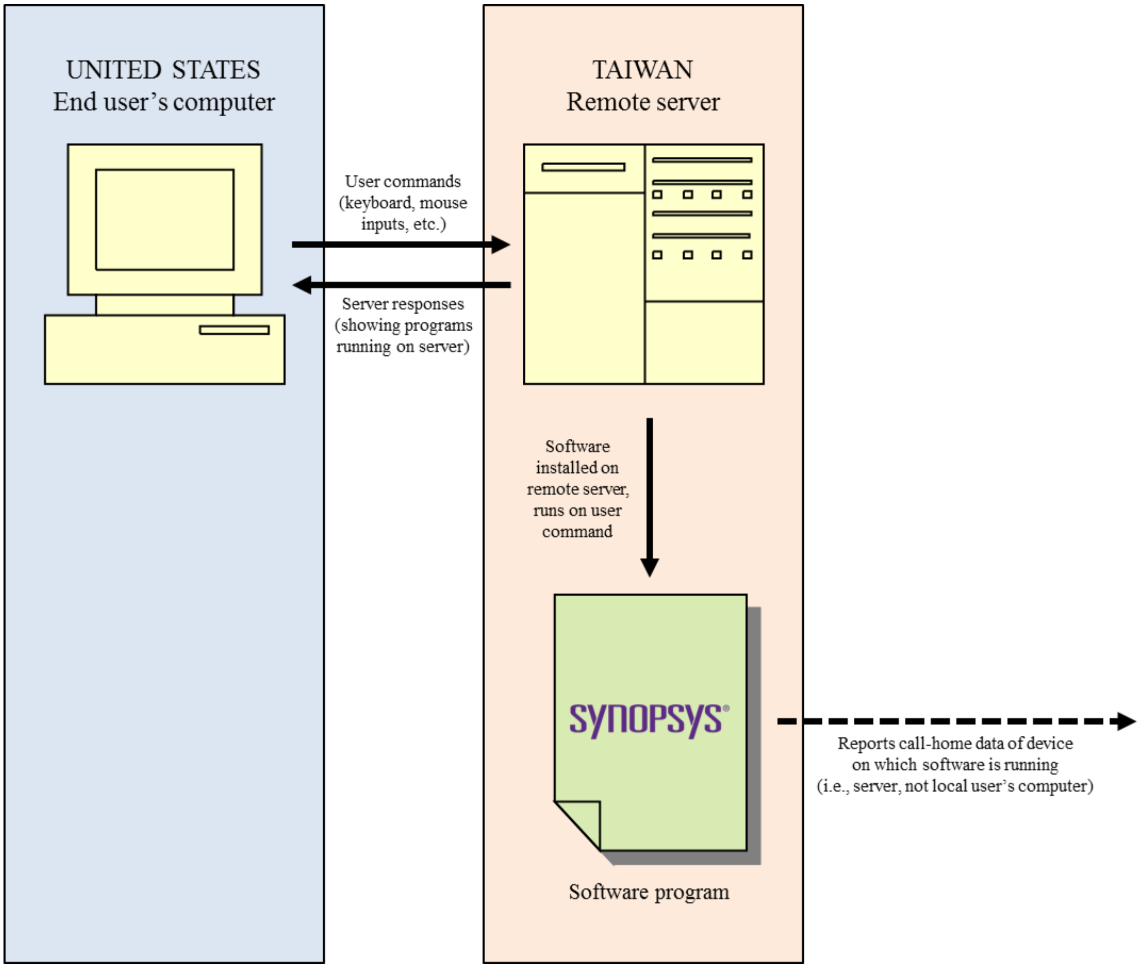
[9] Tsai Decl. – ECF No. 105-5 at 4 (¶ 12).

[10] *Id.* at 4–5 (¶ 13). Synopsys alleges that Ubiquiti installed Synopsys software on other computers in addition to these three servers as well. Jan. 25, 2018 Hr'g.

[11] *See* Nazarian Decl. – ECF No. 105-1 at 4 (¶¶ 9–11); Tsai Decl. – ECF No. 105-5 at 3–5 (¶¶ 7–13).

[12] *See* Tsai Decl. – ECF No. 105-5 at 5–6 (¶ 17).

[13] Jan. 25, 2018 Hr'g.


UNITED STATES
End user's computer
TAIWAN
Remote server
User commands (keyboard, mouse inputs, etc.)
Server responses (showing programs running on server)
Software installed on remote server, runs on user command
SYNOPSYS
Software program
Reports call-home data of device on which software is running (i.e., server, not local user's computer)

Ubiquiti maintains that of the approximately 39,000 alleged circumventions identified in Synopsys's call-home data, only 626 correspond to an IP address originating in the United States.[14] The remaining 38,000 or so call-home entries show an IP address in Taiwan.[15] Synopsys does not dispute these statistics. Ubiquiti then argues that these IP addresses show that "all but 626 of the alleged acts of circumvention took place entirely outside the United States[.]"[16] Synopsys disputes this characterization and argues that if an end user located in the United States remotely connects to a server in Taiwan and then accesses Synopsys software installed on the server, the call-home data would report an IP address originating in Taiwan (the server's IP address), despite

[14] Ubiquiti Br. – ECF No. 105 at 3–4; Taylor Decl. – ECF No. 105-2 at 3 (¶ 6).

[15] Ubiquiti Br. – ECF No. 105 at 4; Taylor Decl. – ECF No. 105-2 at 3 (¶ 6).

[16] Ubiquiti Br. – ECF No. 105 at 2.

the fact that the end user is located in the United States.[17] It is undisputed that at least one U.S.-based Ubiquiti employee, Ching-Han Tsai (who has also been named as an individual defendant), used Synopsys software and that he did so on at least some occasions by logging in remotely from the United States to Ubiquiti servers in Taiwan.[18] According to Synopsys, on at least some of these occasions, the call-home data reported a Taiwanese IP address, not a U.S. IP address.[19]

ANALYSIS

It is important to recall exactly what is before the court. This is a discovery motion. It is not a dispositive motion on the merits of Synopsys's claims. Synopsys is not limited to admissible evidence and need not prove its claims at this juncture. It must only show that, given its claims, the discovery it requests is (1) relevant and (2) proportional to the needs of this case. *See* Fed. R. Civ. P. 26(b)(1). "Information . . . need not be admissible in evidence to be discoverable." *Id.* In deciding whether the plaintiff has made that showing, the court can consider even inadmissible evidence. *Cf.* Fed. R. Evid. 104. *See generally, e.g., Goes Int'l, AB v. Dodur, Ltd.*, No. 14-cv-05666-LB, 2016 WL 427369, at *2 (N.D. Cal. Feb. 4, 2016).

The parties have not presented specifics as to exactly what a forensic inspection would cover, and hence the court does not rule on the relevance (much less on the proportionality or burden) of any particular forensic artifact that may be on Ubiquiti's computers. The court is not issuing a blanket approval of a forensic inspection. But nor may Ubiquiti assert a blanket claim that its Taiwanese computers are not relevant to Synopsys's claims. As discussed below, Ubiquiti's Taiwanese computers and the forensic artifacts on them may be relevant to the case.

[17] Jan. 25, 2018 Hr'g.

[18] Tsai Decl. – ECF No. 105-5 at 5 (¶¶ 14, 16).

[19] Jan. 25, 2018 Hr'g.

1. Ubiquiti's Taiwanese Computers May Be Relevant to Synopsys's DMCA Claims

Among other things, the DMCA provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title" (i.e., a copyrighted work). 17 U.S.C. § 1201(a)(1)(A).[20] At least for the purposes of this discovery motion, the parties do not dispute that (1) Synopsys's software is a copyrighted work, (2) Synopsys's license-key system is a technological measure that controls access to its software, and (3) the use of counterfeit license keys to access and run Synopsys software would be circumventing a technological measure that controls access to a copyrighted work. Instead, the central dispute between the parties is this: when an end user connects to a remote server and, through that remote server, circumvents a technological measure that controls access to a copyrighted work, where is that circumvention deemed to have taken place, and how (if at all) does that affect whether the circumvention gives rise to DMCA liability?

Ubiquiti asserts that the DMCA does not cover circumventions that take place entirely outside the United States, citing *Subafilms, Ltd. v. MGM-Pathe Communications Co.*, 24 F.3d 1088 (9th Cir. 1994) (en banc). There, the Ninth Circuit held that "United States copyright laws do not reach acts of infringement that take place entirely abroad." *Id.* at 1098. Synopsys does not seriously contest that proposition.[21] Ubiquiti also asserts that the DMCA does not cover circumventions that are "initiated" in the United States but are "completed" in a foreign country. Synopsys disputes that proposition.

The parties have not identified (and the court is not aware of) any case that has addressed the question of cross-border circumventions under the DMCA. The parties have therefore drawn

[20] "[T]o 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner," and "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3).

[21] Synopsys notes in passing that traditional copyright law might not apply to a DMCA extraterritoriality analysis, Synopsys Opp'n – ECF No. 109 at 12 n.8, but its primary argument is that "[a]ssuming arguendo for the purposes of this motion that traditional copyright jurisprudence provides the appropriate rubric for analysis of extraterritoriality of the DMCA, Defendants' argument fails on its own terms," *id.* at 12.

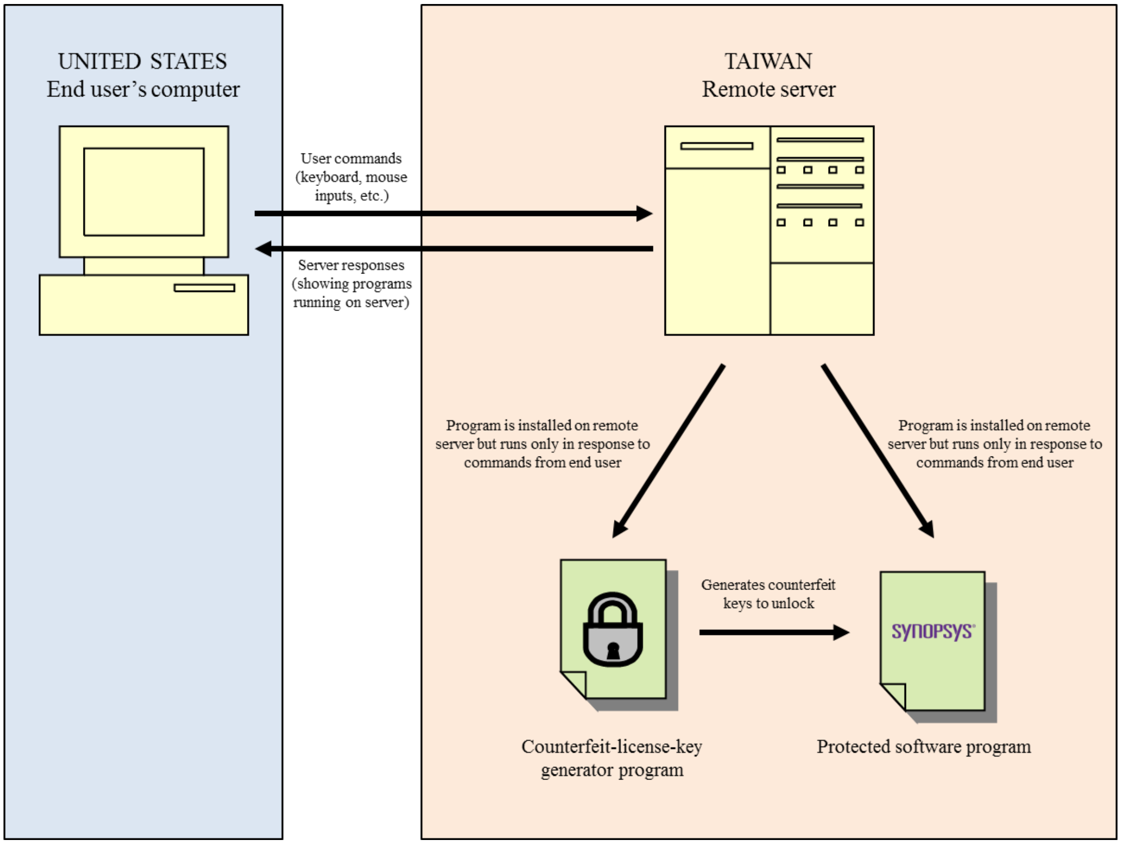
analogies to, and have cited cases addressing, cross-border violations of the exclusive rights granted under the general Copyright Act of 1976. As a threshold matter, it is not clear that cases addressing violations of the general Copyright Act control how a court should address violations of the DMCA. *See generally MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 944–45 (9th Cir. 2016) ("[17 U.S.C.] § 1201(a) prohibits the circumvention of any technological measure that effectively controls access to a protected work and grants copyright owners the right to enforce that prohibition. . . . Historically speaking, preventing 'access' to a protected work in itself has not been a right of a copyright owner arising from the Copyright Act. . . . Accordingly, we read this term as extending a new form of protection[.]").[22] But even assuming that cases addressing violations of the general Copyright Act provide guidance for assessing violations of the DMCA, Synopsys can make a plausible argument under those cases that Ubiquiti's alleged activities are sufficiently related to the United States to give rise to DMCA liability.

The parties dispute exactly how Ubiquiti allegedly circumvented Synopsys's license-key-protection system. Synopsys maintains that Ubiquiti had to pass a license-key check every time it wanted to access and run Synopsys software.[23] The parties have not provided more detail as to what exactly Ubiquiti might have done (and may not know at this juncture). It thus may be helpful to consider a hypothetical set of facts for the purpose of addressing Ubiquiti's legal arguments.

[22] For example, one case cited by the parties, *Allarcom Pay Television, Ltd. v. General Instrument Corp.*, 69 F.3d 381 (9th Cir. 1993), addressed a defendant located in the United States that allegedly broadcast copyrighted television programs via satellite to viewers in Canada. *See id.* at 387. The Ninth Circuit held there that "the potential infringement was only completed in Canada once the signal was received and viewed. Accordingly, U.S. copyright law did not apply[.]" *Id.* But the right at issue in that case was the performance of a copyrighted work, which is not a violation of the Copyright Act unless the performance is public. *See* 17 U.S.C. § 106 ("Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: . . . in the case of . . . motion pictures and other audiovisual works, to perform the copyrighted work *publicly*[.]") (emphasis added). "To perform or display a work 'publicly' means," among other things, "to transmit or otherwise communicate a performance or display of the work . . . to the public," and "[t]o 'transmit' a performance or display is to communicate it by any device or process whereby images or sounds are received beyond the place from which they are sent." 17 U.S.C. § 101. Consequently, the potential copyright infringement in that case arising from the broadcast of television signals (in the United States) was "completed" only when the signal was transmitted and received by the public (in Canada). But it is not a given that the reasoning of that case can be extended to an act of circumvention as defined in the DMCA, which has no analogous "publicly," "transmit," or "received" requirement. *See* 17 U.S.C. § 1201(a)(1).

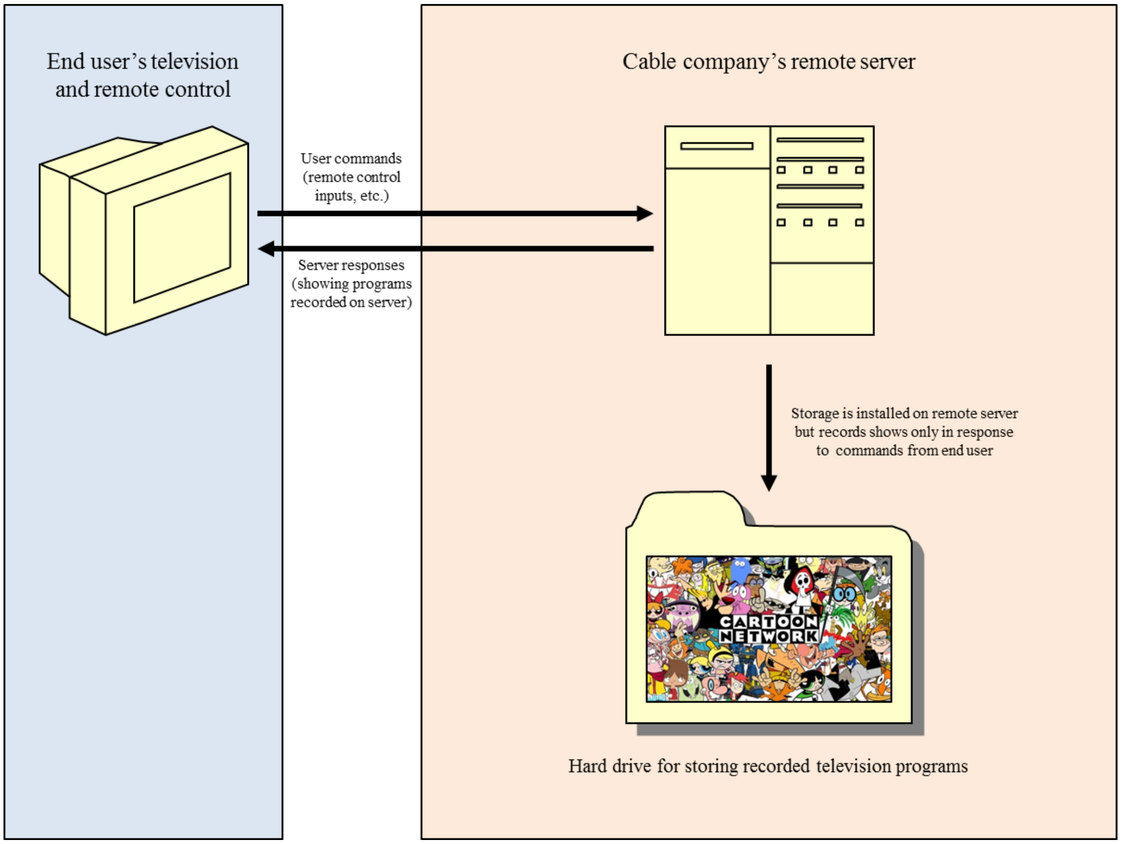
[23] Jan. 25, 2018 Hr'g.

Suppose that to circumvent Synopsys's license-key-protection system, Ubiquiti downloaded a "key generator" program from a "hacker website" onto a Taiwanese computer server.[24] Then, when Ubiquiti employees located in the United States (like Mr. Tsai) wanted to use Synopsys software, they logged onto that remote server and ran the key-generator program, which generated counterfeit license keys that the employees then used to access the software. In this hypothetical, the counterfeit-license-key generator and the use of a counterfeit key to access Synopsys's software run from a remote server in Taiwan, but they run only when an end user in the United States inputs computer commands from his local computer (by typing on his keyboard or moving his mouse), and those commands then are transmitted to the remote server and instruct the server to run the key generator and access Synopsys software.


UNITED STATES
End user's computer
TAIWAN
Remote server
User commands (keyboard, mouse inputs, etc.)
Server responses (showing programs running on server)
Program is installed on remote server but runs only in response to commands from end user
Program is installed on remote server but runs only in response to commands from end user
Generates counterfeit keys to unlock
SYNOPSYS
Counterfeit-license-key generator program
Protected software program

[24] *See* Second Amend. Compl. – ECF No. 73 at 7 (¶ 28) ("Since at least February 2014, Tsai, Ubiquiti, and UNIL have been secretly using counterfeit keys obtained and/or created with tools obtained through hacker websites to circumvent the Synopsys License Key system and access and use Synopsys' EDA software . . . without a valid license.").

As noted above, the parties have not identified any cases where a court has addressed whether a remote act of circumvention, like the one in the hypothetical above, is an act by the remote server in Taiwan outside of the United States, or an act by the end user within the United States. At least one court has addressed the analogous situation, however, of whether a remote act of copying (as opposed to circumvention) is an act by the remote server or by the end user. In *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008), the Second Circuit examined a system involving a remote server for digital video recorders ("DVRs"), analogous to the remote servers at issue here. The system there allowed end users to record television programs by pressing a button on their remote controls. *See id.* at 125. A signal then was sent from the end user's remote control in the user's home to the cable company's server in the company's central facility. *See id.* The server then made a copy of the television program and saved it on a hard drive that the cable company maintained at a remote location. *See id.* at 124.


End user's television and remote control
Cable company's remote server
User commands (remote control inputs, etc.)
Server responses (showing programs recorded on server)
Storage is installed on remote server but records shows only in response to commands from end user
CARTOON NETWORK
Hard drive for storing recorded television programs

The question that the *Cartoon Network* court confronted was "*who* made this copy": the end user or the remote server? *Id.* at 130 (emphasis in original). The court answered by holding that "copies produced by the [remote storage]-DVR system are 'made' by the RS-DVR customer," not the remote server, *id.* at 133, because "the person who actually presses the button to make the recording, supplies the necessary element of volition," *id.* at 131.[25]

By analogy, just as an end user who presses a button and thereby inputs the command to record a television program is making a copy of the program under the Copyright Act (even if that television program is saved on a remote server), an end user who inputs commands to use a counterfeit license key to bypass a software-protection system may be engaging in an act of circumvention under the DMCA (even if that counterfeit key and software are installed on a remote server). If that end user is located in the United States, his circumvention might give rise to DMCA liability despite its cross-border nature. *See generally Automattic Inc. v. Steiner*, 82 F. Supp. 3d 1011, 1028 (N.D. Cal. 2015) (holding in the context of a different DMCA provision that "the application of the [DMCA] is not extraterritorial" when "key elements of the cause of action were performed in [the United States]").[26]

Ubiquiti, for its part, proposes an alternative hypothetical where, instead of using a license-key-generator program, some person or persons outside the United States "hacked" the Synopsys software to remove the license-key-protection system entirely, so that after that one act of

[25] The Ninth Circuit cited *Cartoon Network* with approval in *Fox Broadcasting Company, Inc. v. Dish Network L.L.C.*, 747 F.3d 1060 (9th Cir. 2014), another copyright case involving DVRs. Unlike the DVRs in *Cartoon Network*, the DVRs in *Fox* made copies of television programs on local hard drives in set-top boxes in the users' homes, not on remote hard drives on a central server, *see id.* at 1065, and hence the issue of remote connections was not present in that case in the same way it was in *Cartoon Network*. Regarding the underlying question of "who made the copies," however, the Ninth Circuit cited *Cartoon Network* and held that because the DVR system "creates the copy only in response to the user's command. . . . the district court did not err in concluding that the user, not [the DVR system], makes the copy." *Id.* at 1067; *accord Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 670 (9th Cir. 2017) ("Operating a system used to make copies at the user's command does not mean that the system operator, rather than the user, caused copies to made.") (internal brackets omitted) (quoting *Fox*, 747 F.3d at 1067).

[26] Whether the remote server, in addition to the end user, also is engaging in circumvention is a question the court need not answer here. Additionally, the court need not answer whether the owner of the remote server, by allowing users to connect and run key-generator programs on its server, might be violating other DMCA provisions, such as the DMCA's prohibition on trafficking in services that are primarily designed or produced for the purpose of circumvention, 17 U.S.C. §§ 1201(a)(2), 1201(b)(1).

circumvention, the software never again checked any license keys.[27] Ubiquiti users located in the United States then ran Synopsys software only after this hacking was completed, so those U.S. users were never prompted for a license key and never generated a counterfeit license key themselves. Ubiquiti argues that in that case, no DMCA liability would attach because in this second hypothetical (unlike the first), the act of circumvention took place entirely outside the United States, and the U.S. users' subsequent *access* to the Synopsys software, separate and apart from the acts of *circumvention*, does not violate the DMCA.[28]

The court need not decide at this juncture whether Ubiquiti would have no DMCA liability in that particular fact scenario. In the context of the current discovery dispute, it is enough to say that there are at least some fact scenarios (such as the first hypothetical) in which Ubiquiti may have potential DMCA liability, and hence discovery is necessary to determine what the actual facts are. Certainly, the factual record is too embryonic to rule that Ubiquiti's Taiwanese computers cannot be relevant to a valid DMCA claim as a matter of law. *Cf. Goes*, 2016 WL 427369, at *2. What exactly Ubiquiti did and did not do vis-à-vis Synopsys's license-key-protection system may matter, and discovery into Ubiquiti's Taiwanese computers is thus relevant to determine exactly what Ubiquiti did and did not do.

2. The "Server Test" That Ubiquiti Cites Is Inapposite

Ubiquiti argues that in *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007), the Ninth Circuit established a "server test," and that under this test, "it is clear that the site of the violative act (the alleged use of 'counterfeit' license keys to circumvent Synopsys' license-key system) are the servers that actually hosted Synopsys software — because that is the only place where the act *could* be completed — and not an employee computer that remotely initiated the act

[27] Jan. 25, 2018 Hr'g.

[28] *See* Ubiquiti Reply Br. – ECF No. 110 at 4 & n.3 (arguing that "the act of accessing a copyrighted work *after* a technological measure has been circumvented, as opposed to the *circumvention itself*," does not violate 17 U.S.C. § 1201(a)(1)) (emphasis in original) (citing *MGE UPS Sys., Inc. v. GE Consumer & Indus., Inc.*, 622 F.3d 361, 366 (5th Cir. 2010)).

or where the displayed results could be viewed."[29] The "server test" in *Perfect 10*, however, does not address the question of distinguishing between end users and remote servers. Rather, the situation in *Perfect 10* involved connections between *three* parties — end users, third-party servers hosting copyrighted material, and search engines that did not themselves host copyrighted material but that linked end users to the third-party servers that did host copyrighted material — and the "server test" was a test to distinguish between the hosting third-party servers and the non-hosting search engines. The test did not address activities by end users and therefore is inapposite here.

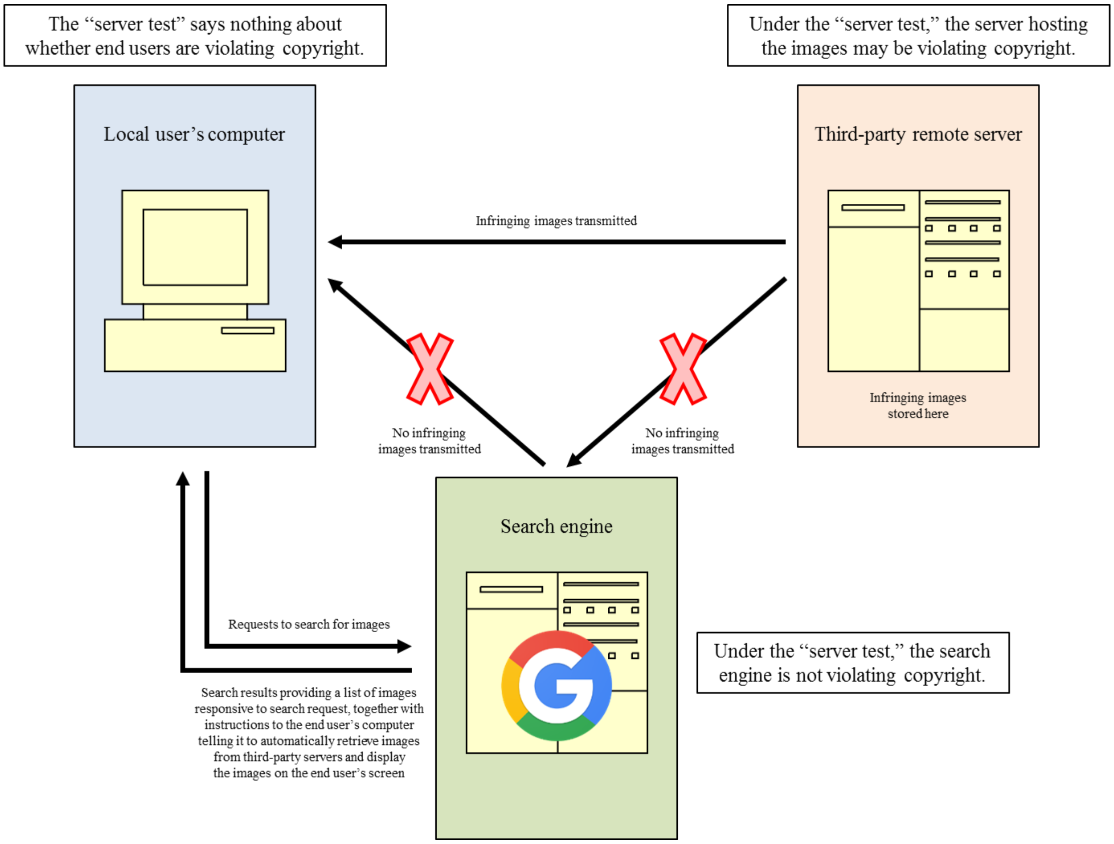
The plaintiff in *Perfect 10* was a copyright holder of photographic images that brought a copyright-infringement claim against the internet search engine Google, alleging (among other things) that copies of its photographs appeared in Google search results, *see id.* at 1155–56, and that Google was thereby violating its exclusive right to publicly display and distribute its photographs, *see id.* at 1159. Google responded that while the photographs in question appeared on users' screens in Google search results, the photographs actually were being transmitted directly from third-party servers to end users, without ever going through Google, and hence Google was not the party that was displaying or distributing the images. *See id.* at 1156 ("Google . . . does not communicate the images to the user; Google simply provides [computer] instructions directing a user's browser to access a third-party website. . . . Thus, the user's window appears to be filled with a single integrated presentation of the full-size image, but it is actually an image from a third-party website framed by information from Google's website.").

The district court and the Ninth Circuit applied a "server test" to determine which party — the remote server or *Google* (not the remote server or the end user) — was violating the plaintiff's copyright. *Id.* at 1159. The courts held that under the "server test," only a server that actually stored the photographs as electronic information and "serves that electronic information directly to the user ('i.e., physically sending ones and zeroes over the Internet to the user's browser')" could infringe the copyright holder's rights, whereas a search engine like Google "that does not store and

[29] Ubiquiti Br. – ECF No. 105 at 10 (emphasis in original).

United States District Court
Northern District of California

serve the electronic information to a user" did not infringe on the copyright owner's rights. *Id.* at 1159 (citations and internal brackets omitted).


The "server test" says nothing about whether end users are violating copyright.
Under the "server test," the server hosting the images may be violating copyright.
Local user's computer
Third-party remote server
Infringing images transmitted
Infringing images stored here
No infringing images transmitted
No infringing images transmitted
Search engine
Requests to search for images
Search results providing a list of images responsive to search request, together with instructions to the end user's computer telling it to automatically retrieve images from third-party servers and display the images on the end user's screen
Under the "server test," the search engine is not violating copyright.

Contrary to Ubiquiti's claims, nothing in the "server test" holds that when an end user initiates a copyright violation through the use of a remote server, the violation occurs only at the site of the server and does not, as a matter of law, occur at the site of the end user. Consequently, the "server test" does not address the legal questions presented here, and nothing in the test alters the conclusion that Ubiquiti's Taiwanese servers may be relevant to Synopsys's DMCA claims, as discussed above.[30]

[30] Elsewhere in the *Perfect 10* opinion — outside of the context of the "server test" — the Ninth Circuit considered whether end users might be engaging in a *separate* act of copyright infringement if they downloaded the images and saved copies of them on their computers. It noted, however, that there was no evidence in the record to support this claim. *Id.* at 1169. The Ninth Circuit also considered — again, outside the context of the "server test" — whether end users' web browsers made "cache" copies of the images and whether that might constitute a separate act of copyright infringement by the end users, but then held that caching constituted a fair use. *Id.* at 1169–70. These discussions of

3. Ubiquiti's Taiwanese Computers May Be Relevant to Synopsys's Other Claims

In addition to DMCA claims, Synopsys brings other claims, including claims for fraud. Among other things, Synopsys alleges that Ubiquiti represented that it wanted to legitimately license Synopsys software, that Ubiquiti made these representations to induce Synopsys to provide Ubiquiti with copies of its software and temporary license-key files[31] and to induce Synopsys to show Ubiquiti how to configure license-key files,[32] and that these representations were false when they were made.[33] Ubiquiti's Taiwanese computers may be relevant to these claims. For example, if there were forensic evidence on Ubiquiti's computers that Ubiquiti had already obtained counterfeit license keys or key generators when it made those representations to Synopsys, that evidence would be relevant to Ubiquiti's knowledge of the falsity of its representations at the time that they were made, and hence relevant to Synopsys's fraud claims.

CONCLUSION

In sum, the court holds that Ubiquiti may not per se exclude its Taiwanese computers from the scope of discovery merely because they are located outside the United States.

This order should not be interpreted, however, as a blanket approval of any and all forensic inspections of Ubiquiti's computers. As the court previously advised the parties,[34] discovery, including any forensic inspections, must comply with the standard discovery factors, including proportionality, burden, and the defendants' legitimate interests in maintaining the integrity of their systems and the confidentiality of their data. If the parties have not yet reached an agreement, they must meet and confer regarding an appropriate inspection protocol. If the parties cannot agree on a solution, they may raise issues in a joint discovery-dispute letter brief that complies with the

possible separate acts of copyright violation by end users were not related to the "server test" that Ubiquiti cites here.

[31] *See, e.g.*, Second Amend. Compl. – ECF No. 73 at 10–14 (¶¶ 41–45, 49–52).

[32] *See, e.g.*, *id.* at 12 (¶¶ 46–47).

[33] *See, e.g.*, *id.* at 10–14 (¶¶ 42, 47, 51).

[34] Order – ECF No. 104 at 5–6.

undersigned's standing order.[35] If the parties request an additional hearing, the parties must submit their joint letter brief no later than one full week before the hearing date. The court generally holds hearings on Thursdays at 9:30 a.m.

IT IS SO ORDERED.

Dated: January 29, 2018

LAUREL BEELER
United States Magistrate Judge

[35] Standing Order – ECF No. 104-1.